Telepathwords : empêcher les mots de passe faibles en lisant dans l'esprit des individus

Nicola Spanti

Janvier 2017

Système d'authentification

- Utilisateurs et/ou utilisatrices
- Administrateur(s) et/ou administratrices systèmes
- Attaquant(s) et/ou attaquante(s)

Règles de mots de passe

- Définis par le(s) administrateur(s) et/ou administratrices systèmes
- Longueur
- Casse, nombre, symbole

Mais

- P@$$word
- Thisismypassword
- Azerty !23456

But

- Protéger les organisations
- Beaucoup d'utilisateurs et/ou utilisatrices
- Mot de passe le plus faible pour s'introduire

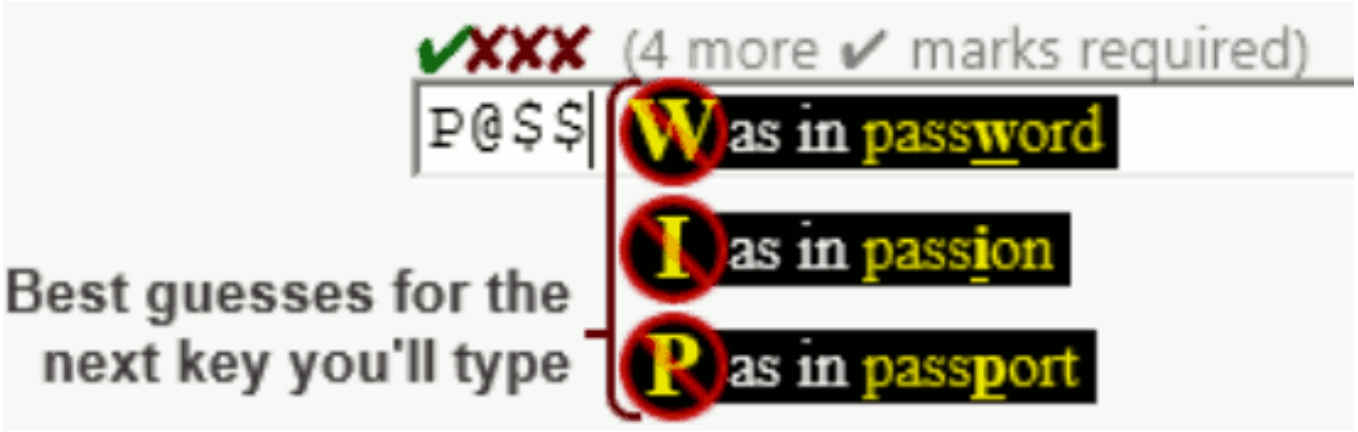
Telepathwords

- Détection des mots de passe faibles
- Information en temps réel

Cela marche :

- Meilleur sécurité
- Confort similaire après la définition du mot de passe

Exemple



L'interface graphique proposée

Algorithmes de prédiction

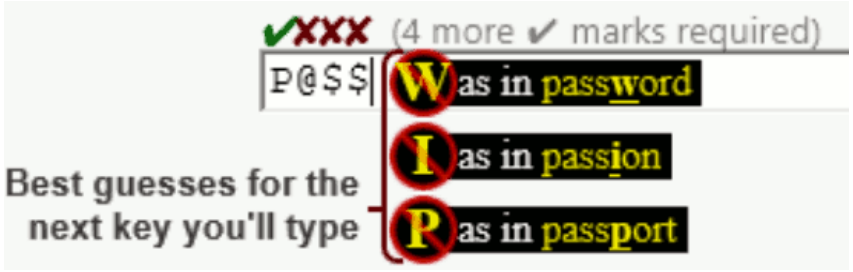
- les séquences de caractères courantes
  - "prédi" $\rightarrow$ "re" ou "iction"
  - "vie" $\rightarrow$ "privée" ou "intime"
  - "pa1234ssword" et "12x34y678z9"
  - "P@$$word"
- la proximité des caractères sur un clavier
  - "123456" ou "azerty",
  - Disposition du clavier :-(
- les répétitions
  - "xyabcabcabc"
  - "abcdefabc"
- les mots écrits un caractère sur 2
  - "p*a*s*s*w*o*r*d"
  - "ppaasswwoorrdd"

Règles "classiques"

- basic8 : 8 caractères au moins
- 3class8 : basic8 + 3 classes parmi 4 (minuscules, majuscules, chiffres, symboles)
- 3class12 : 3class8 pour 12 caractères
- 3class8-d : 3class8 sans mot d'un dictionnaire

Règles de *Telepathwords*

- Au moins 6 caractères non prédis (dont le 1ercaractère)
- Différence
  - telepath-v : visible par défaut
  - telepath : caché par défaut



Comparaisons : conditions de l'étude

- Règle aléatoire
- Questions (règle, habitudes sur les mots de passe, localisation géographique)
- Demande du mot de passe
- Demande du mot de passe, 2 jours après

Comparaisons : résultats

- temps d'enrollement plus long
- difficulté perçue pour respecter la règle similaire à 3class8-d (et plus grande que les autres)
- perception de sécurité similaire similaire à 3class12 et 3class8-d
- aide visuelle meilleure
- 3class12, telepath et telepath-v utiles pour un mot de passe robuste (d'après les individus)
- le plus faible est moins faible avec *Telepathwords* que les autres

Conclusions

- classes de caractères sans effet ou presque (avec les métriques utilisées)
- coût à la création
- *Telepathwords* efficace pour faire monter vers le haut le mot de passe le plus faible
- pas de coût supplémentaire de mémorisation